DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents

June 3 - 30, 2013

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000090102	Missing/Stolen Equipment	VISN 07 Birmingham, AL	6/3/2013		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0590803	6/3/2013	INC000000287357	N/A	N/A	N/A		

Incident Summary

On Monday 06/03/13, a Report of Survey was delivered to the Information Security Officer (ISO) indicating that a PC used in a patient room to deliver entertainment content and educational videos as part of the GetWellNetwork was missing. The device was not encrypted, but was not connected to the VA LAN and was not used to store any patient information.

The ISO notified facility leadership, VA Police, Chief Information Officer, and the Privacy Officer.

Incident Update

06/03/13:
There was no personally identifiable information (PII) or protected health information (PHI) stored on the computer. The investigation of the theft is ongoing.

0610/13:
The ISO is waiting on a Police report to be completed.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000090106	Mishandled/ Misused Physical or Verbal Information	VBA Atlanta, GA	6/3/2013	7/10/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0590808	6/3/2013	INC000000287372	N/A	N/A	N/A	1	

Incident Summary

Veteran A received a letter containing Veteran B's claim information. The letter had Veteran B's Social Security Number, address, compensation and pension claim rating, along with what service connected issues Veteran B is currently approved/denied.

Incident Update

06/03/13:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 122 Mis-Mailed incidents this reporting period. Because of repetition, the other 121 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

Employee was counseled and trained on records management procedures to prevent reoccurrence.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000090152	Mishandled/ Misused Physical or Verbal Information	VISN 23 Minneapolis, MN	6/4/2013	6/13/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0590862	6/4/2013	VANSOC0590862	N/A	N/A	N/A	2	

Incident Summary

A nursing assistant left two Blood Product slips on a cart in a public hallway while in the restroom.

Incident Update

06/04/13:
Two patients will be sent letters offering credit protection services due to full name and full SSN being exposed.

06/19/13:
This was determined to be HITECH reportable by VHA Privacy Office.

NOTE: There were a total of 102 Mis-Handling incidents this reporting period. Because of repetition, the other 101 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

This incident is being sent to Human Resources Management Service (HRMS) for action. The employee is required to re-take privacy training.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000090186	Missing/Stolen Equipment	VISN 23 Iowa City, IA	6/4/2013		Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0590900	6/4/2013	INC000000287873	N/A	N/A	N/A		

Incident Summary

During a routine equipment inventory, four computers were unable to be located. The four computers consisted of two laptops and two PC towers. IT Service Delivery and Engineering (SD&E) reported one of the laptops may not have been configured with encryption and had not connected to the VA Network. At this time there is no indication of a VA data loss or that personally identifiable information (PII) or protected health information (PHI) was stored on any of the device hard drives. The VA Police have been notified and a Report of Survey has been started.

Incident Update

06/06/13:
One laptop has been located and is still in operation supporting a bio-med device. The bio-med device laptop was on the incorrect Equipment Inventory Listing (EIL). The laptop that is still unaccounted for is encrypted. There is no indication that PII or PHI was on any of the missing devices.

NOTE: There were a total of 2 IT Equipment Inventory Incidents this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000090429	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Dallas, TX	6/10/2013	6/12/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0591169	6/10/2013	INC000000289120	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the Central Texas-Temple Medical Center and a replacement has been requested for Patient B. Dallas Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employee will be counseled and retrained in proper packing procedures.

Incident Update

06/10/13:
Patient B will be sent a notification letter.

06/19/13:
This was determined to be non-HITECH reportable by VHA Privacy Office.

NOTE: There were a total of 3 Mis-Mailed CMOP incidents out of 6,314,591 total packages (9,377,073 total prescriptions) mailed out for this reporting period. Because of repetition, the other 2 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter.

Resolution

The CMOP employee was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000090559	Missing/Stolen Equipment	VISN 22 Long Beach, CA	6/12/2013	6/27/2013	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0591292	6/12/2013	INC000000289974	N/A	N/A	N/A	17	

Incident Summary

A VA unencrypted laptop has been reported missing. All evidence points to the fact that this laptop may have been removed by an unauthorized individual. The VA Police report is forthcoming.

Incident Update

06/17/13:
The laptop was included as part of a Super Dimension I-Logic CT Guided Biopsy Navigational System package and was only used in conjunction with this medical device. According to reporting Respiratory Therapy staff, personally identifiable information (PII) and protected health information (PHI), including name, full SSN and CT images of 17 patients were stored on the laptop at the time laptop turned up missing. From the time the medical device went into use, which was approximately 2 months, no data scrubbing routine was implemented. According to reporting physician, the laptop was last seen on 05/07/13. The laptop turned up missing from the reporting physician's office. It was never on the VA network. It was reported to the VA Police.

Seventeen patients will receive a letter offering credit protection services.

Resolution

The VA Police Department entered the loss into the Police database system which alerts the Regional Police authorities. The Information Security Officer (ISO) is working with health care group in order to reinforce security controls and policies.

Total number of Internal Un-encrypted E-mail Incidents	75
Total number of Mis-Handling Incidents	102
Total number of Mis-Mailed Incidents	122
Total number of Mis-Mailed CMOP Incidents	3
Total number of IT Equipment Inventory Incidents	2
Total number of Missing/Stolen PC Incidents	1
Total number of Missing/Stolen Laptop Incidents	10 (8 encrypted)
Total number of Lost BlackBerry Incidents	24
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0